UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/938,489	08/27/2001	James Malcolm Vignoles	550-261	2875

23117 7590 08/05/2005		EXAMINER
NIXON & VANDERHYE, PC		SCHUBERT, KEVIN R
901 NORTH GLEBE ROAD, 11TH FLOOR		
ARLINGTON, VA 22203	ART UNIT	PAPER NUMBER
	2137	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

/1/

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 July 2005_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-6,8-18,20-30 and 32-36_ is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-6,8-18,20-30 and 32-36_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All   b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Claims 1-6,8-18,20-30, and 32-36 have been considered. The examiner notes that he

appreciates the applicant's time and concerted efforts in the interview conducted 7/18/05.

5   *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as
> set forth in section 102 of this title, if the differences between the subject matter sought to be
10 > patented and the prior art are such that the subject matter as a whole would have been obvious
> at the time the invention was made to a person having ordinary skill in the art to which said
> subject matter pertains. Patentability shall not be negatived by the manner in which the invention
> was made.

15

Claims 1-6,8-9,11-18,20-21,23-30,32-33, and 35-36 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Waldin, U.S. Patent No. 6,094,731, in view of Tamaru, U.S. Patent No. 4,788,637, in

further view of Hoene, U.S. Patent No. 2002/0199116.

20   As per claims 1,13, and 25, the applicant describes a computer program product with the

following limitations which are met by Waldin in view of Tamaru in further view of Hoene:

a) reading logic operable to read an update status field associated with a computer file to be

scanned by a current malware scanner, said update status field being indicative of an update status of a

previous malware scanner that has scanned said computer file and associated said update status field

25   with said computer file (Waldin: Col 6, lines 25-36);

b) comparison logic operable to compare said update status of said previous malware scanner

with an update status of said current malware scanner (Waldin: Col 6, lines 25-36);

c) alert issuing logic operable if said update status of said current malware scanner does not

match said update status of said previous scanner to issue an update status alert indicative of an out-of-

date update status for whichever one of said current malware scanner and said previous malware

scanner has a most out-of-date update status (Tamaru: Figs 6 and 7);

   d) change logging logic operable to log changes to said update status field to create a change

history in an update status tracking database to enable identification of weaknesses within update status

5   management based on the change history (Hoene: [0025]; [0036]);

   Waldin discloses parts a and b above. Waldin does not disclose part c, "an update status alert

indicative of an out-of-date update status for whichever one of said current malware scanner and previous

malware scanner has a most out-of-date update status". In other words, Waldin does not disclose a

means to communicate to the originating computer that he has an old version of a scanning program.

10 Tamaru discloses a system between an originating computer and a recipient computer in which a

message is sent between the two computers which includes a header indicating the version of a program

the sending computer is using. The recipient computer compares the version with the version it is

currently using and sends an alert indicative of whichever computer has the most outdated version of the

program.

15   It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

combine the ideas of Tamaru with those of Waldin because doing so allows the originating computer to

know if it has an outdated scanner program so that it can find a means to retrieve a newer program.

   Waldin in view of Tamaru disclose parts a through c above. However, Waldin in view of Tamaru

do not disclose logging data related to the virus scan in an update status tracking database to enable

20 identification of weaknesses. In the interview conducted 7/18/05, the examiner called the applicant to

clarify what exactly is meant by identification of weaknesses. The applicant referred the examiner to the

Specification (see Spec page 9, lines 14-16) and noted that patterns of weaknesses are established by

cumulatively tracking records of virus scan data. This tracking allows an administrator to ascertain

particular systems that regularly incur virus infections and/or regularly fail to maintain an up-to-date virus

25 scan.

Hoene teaches this idea in a system which includes a quarantine monitor to identify patterns of

weaknesses by cumulatively tracking virus scan information presented to it by network clients. The

examiner notes the following lines of Hoene:

"Quarantine monitor comprises a registry for tracking virus-infected client computers and which
5   virus they each were infected with, and when the infection occurred. Quarantine monitor also tracks
virus-susceptible client computers, such as those without an up-to-date virus scan and/or those with
disabled virus protector. This information may be tracked cumulatively and used for detecting patterns in
virus infection, detection, and eradication" [0025].

10   It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

combine the ideas of Hoene with those of Waldin in view of Tamaru and log the virus scan data in a

database because doing so allows an administrator to cumulatively track virus scan information in the

system.

15   As per claims 2,14, and 26, the applicant describes the computer program product of claims 1,13,

and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is

met by Waldin:

Wherein said update status field is included as a property field within said computer file (Col 5,

lines 21-27);

20   The property field is the header field.

As per claims 3-4,15-16, and 27-28, the applicant describes the limitations of claims 1,13, and 25,

which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by

Waldin:

25   Wherein said update status field is included within an update status file passed together and

associated with said computer file between malware scanners (Col 5, lines 21-27).

As per claims 5,17, and 29, the applicant describes the limitations of claims 4,16, and 28, which

are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by

30   Waldin:

Wherein said combined file is a file compressed combination of said update status file and said computer file (Col 6, lines 1-9);

The update status file is compressed by hashing and the hash is combined with the computer file to form a compressed combination of the update status file and the computer file.

5

As per claims 6,18, and 30, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by Tamaru:

Wherein, if said malware scanner has a less out-of-date update status than said previous

10   malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner (23 of Fig 2; Col 2, line 65 to Col 3, line 7);

The update status field is the version number. If current station 2 has a more recent program than station 1, the update status field (23 of Fig 2) is changed to correspond to the current station 2's program. The applicant should note that though Tamaru specifically references a communication control

15   program and the applicant references a scanner, the particular type of program is an obvious change in the system.

As per claims 8,20, and 32, the applicant describes the limitations of claims 1,13, and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by

20   Tamaru:

Wherein said update status alert includes one or more of:

a) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

b) an administrator alert issued to an administrator of whichever one of said current malware

25   scanner and said previous malware scanner has a most out-of-date update status (3 of Fig 1);

The administrator can be the controller of the stations.

As per claims 9,21, and 33, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by Waldin:

Wherein said computer file is an e-mail attachment (Col 5, lines 21-27).

5

As per claims 11,23, and 35, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by Waldin:

Wherein said update status field includes one or more of:

10   (i) a malware scanner computer program product identifier;

(ii) a computer hardware identifier;

(iii) a scanner engine program version identifier (Col 6, lines 31-36);

(iv) a malware definition data version identifier.

15   As per claims 12,24, and 36, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru in view of Hoene, with the following limitation which is met by Waldin:

Wherein said malware scanner server to detect one or more of:

(i) a computer virus (Col 2, lines 6-7);

20   (ii) a Trojan computer program;

(iii) a worm computer program;

(iv) a banned computer program.

Claims 10,22, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waldin in

25   view of Tamaru in further view of Hoene in further view of Grupe, U.S. Patent Application Publication No. 2002/0194487.

As per claims 10,22, and 34, the applicant describes the method of claims 1,13, and 25, which are met by Waldin in view of Tamaru in further view of Hoene, with the following limitation which is met by Grupe:

Wherein said current malware scanner and said previous malware scanner are part of a tiered

5   malware scanner [0017];

Waldin in view of Tamaru in further view of Hoene disclose all the limitations of claims 1,13, and 25. However, Waldin in view of Tamaru in further view of Hoene fail to disclose that the scanning environment is tiered. Grupe discloses a similar scanning system which takes place in a tiered environment. It would have been obvious to one of ordinary skill in the art at the time the invention was

10   filed to combine the ideas of Grupe with those of Waldin in view of Tamaru in further view of Hoene and incorporate the use of a tiered environment in the case where different computers have different scanning responsibilities.

Response to Arguments

15   Applicant's arguments with respect to amended claims 1,13, and 25 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office

20   action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

25   shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX

MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should

be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally

5   be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where

this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application

10   Information Retrieval (PAIR) system. Status information for published applications may be obtained from

either Private PAIR or Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)

at 866-217-9197 (toll-free).

15   EMMANUEL L. MOISE
       KS   SUPERVISORY PATENT EXAMINER